

AMENDMENT(S) TO THE CLAIMS

1  
2  
3       1. (currently amended): A method for generating a permission grant set for  
4 a code assembly received from a resource location, the method comprising:

5           receiving a security policy specification defining a plurality of code groups,  
6 each code group being associated with a code-group permission set;

7           receiving evidence associated with the code assembly;

8           evaluating the evidence relative to the code groups to determine  
9 membership of the code assembly in ~~one~~ two or more of the code groups; and

10          generating the permission grant set based on ~~one~~ two or more code-group  
11 permission sets, each code-group permission set of the ~~one~~ two or more code-  
12 group permission sets being associated with a code group in which the code  
13 assembly is a member.

14  
15       2. (currently amended): The method of claim 1 wherein the generating  
16 operation comprises:

17           dynamically generating a code-group permission set based on permissions  
18 associated with the ~~one~~ two or more code groups.

19  
20       3. (original): The method of claim 1 wherein the generating operation  
21 comprises:

22           computing a logical set operation on code-group permission sets associated  
23 with the code groups in which the code assembly is a member to generate the  
24 permission grant set.

1           4. (original): The method of claim 3 wherein the computing operation  
2 comprises:

3           computing the logical set operation based on order values associated with  
4 the code groups.

5  
6           5. (original): The method of claim 1 wherein the generating operation  
7 comprises:

8           computing a union of the code-group permission sets associated with code  
9 groups in which the code assembly is a member to generate the permission grant  
10 set.

11  
12           6. (original): The method of claim 1 wherein the security policy  
13 specification further defines at least one code group collection associated with the  
14 plurality of code groups and the generating operation comprises:

15           selecting a code-group permission set associated with an individual code  
16 group of the code group collection in which the code assembly is a member to  
17 generate the permission grant set.

18  
19           7. (original): The method of claim 6 wherein the security policy  
20 specification defines the at least one code group collection as a code group  
21 hierarchy.

1           8. (original): The method of claim 6 further comprising:

2           an exclusive property associated with the single code group indicating that  
3 the code-group permission set associated with the single code group is to be  
4 selected to generate the permission grant set.

5  
6           9. (original): The method of claim 8 further comprising:

7           an exclusive property associated with the single code group indicating that  
8 no code-group permission set associated with a code group existing below the  
9 single code group in a code group hierarchy is to be used to generate the  
10 permission grant set.

11  
12           10. (original): The method of claim 1 wherein the security policy  
13 specification further defines a policy level associated with the plurality of code  
14 groups, and the generating operation comprises:

15           computing a union of the code-group permission sets associated with code  
16 groups in which the code assembly is a member to generate a policy-level  
17 permission set; and

18           generating the permission grant set based on the policy-level permission set.  
19  
20  
21  
22  
23  
24  
25

1           **11.** (original): The method of claim 1 wherein the security policy  
2 specification further defines at least one code group collection associated with the  
3 plurality of code groups and a policy level associated with the at least one code  
4 group collection, and the generating operation comprises:

5           selecting a code-group permission set associated with an individual code  
6 group of the code group collection in which the code assembly is a member to  
7 generate a policy-level permission set; and

8           generating the permission grant set based on the policy-level permission set.

9  
10           **12.** (original): The method of claim 1 wherein the security policy  
11 specification further defines a plurality of policy levels, each policy level being  
12 associated with the plurality of code groups, and the generating operation  
13 comprises:

14           selecting, for each policy level, a code-group permission set associated with  
15 an individual code group in the code groups of the policy level in which the code  
16 assembly is a member to generate a corresponding policy-level permission set; and

17           merging the corresponding policy-level permission sets to generate the  
18 permission grant set.

19  
20           **13.** (original): The method of claim 12 wherein the merging operation  
21 comprises:

22           computing an intersection of the corresponding policy-level permission sets  
23 associated with each policy level.  
24  
25

1       **14.** (original): The method of claim 1 wherein the security policy  
2 specification further defines a plurality of policy levels, each policy level being  
3 associated with a plurality of code groups, and the generating operation comprises:

4           computing, for each policy level, a union of the code-group permission sets  
5 associated with code groups of the policy level in which the code assembly is a  
6 member to generate a corresponding policy-level permission set; and

7           merging the corresponding policy-level permission sets to generate the  
8 permission grant set.

9  
10       **15.** (original): The method of claim 14 wherein the merging operation  
11 comprises:

12           computing an intersection of the corresponding policy-level permission sets  
13 associated with each policy level.

14  
15       **16.** (original): The method of claim 1 wherein the security policy  
16 specification further defines a plurality of ordered policy levels associated with the  
17 plurality of code groups, such that a first policy level defines a more restrictive  
18 security policy than a second policy level.

19  
20       **17.** (original): The method of claim 1 further comprising:  
21           extracting from the security policy specification a membership criterion for  
22 a code group in the plurality of code groups.

1       **18.** (original): The method of claim 17 wherein the evaluating operation  
2 comprises:

3       extracting one or more trust characteristics from the evidence;  
4       evaluating the trust characteristics relative to the membership criterion; and  
5       identifying the code assembly as a member of the code group, if the one or  
6 more trust characteristics satisfy the membership criterion.

7  
8       **19.** (original): The method of claim 1 further comprising:  
9       extracting from the security policy specification a code-group permission  
10 set for each code group in the plurality of code groups.

11  
12       **20.** (original): The method of claim 1 wherein the security policy  
13 specification further describes at least one code group hierarchy associated with  
14 the plurality of code groups, each code group collection including a parent code  
15 group, and further comprising:

16       extracting from the security policy specification a definition of at least one  
17 child code group of the parent code group in the at least one code group collection.

18  
19       **21.** (original): The method of claim 20 wherein the evaluating operation  
20 comprises:

21       determining whether the code assembly is a member of the parent code  
22 group; and

23       determining whether the code assembly is a member of the at least one child  
24 code group, if the code assembly is a member of the parent code group.

25

1           22. (previously presented): The method of claim 1 further comprising:  
2           performing verification on the code assembly;  
3           detecting a verification failure of the code assembly in the operation of  
4 performing verification; and  
5           determining based on the permission grant set whether the code assembly  
6 may be executed despite the verification failure.

7  
8           23. (previously presented): The method of claim 1 further comprising:  
9           determining based on the permission grant set that a step of a verification  
10 process is unnecessary;  
11           communicating to a verification module that the step of the verification  
12 process may be bypassed;  
13           performing the verification process on the code assembly with the  
14 verification module; and  
15           bypassing the step of the verification process, responsive to the  
16 communicating operation.

1           24. (currently amended): A computer data signal embodied in a carrier  
2 wave by a computing system and encoding a computer program for executing a  
3 computer process generating a permission grant set for a code assembly received  
4 from a resource location, the computer process comprising:

5           receiving a security policy specification defining a plurality of code groups,  
6 each code group being associated with a code-group permission set;

7           receiving evidence associated with the code assembly;

8           evaluating the evidence relative to the code groups to determine  
9 membership of the code assembly in ~~one~~ two or more of the code groups; and

10          generating the permission grant set based on ~~one~~ two or more code-group  
11 permission sets, each code-group permission set of the ~~one~~ two or more code-  
12 group permission sets being associated with a code group in which the code  
13 assembly is a member.



1           **25.** (currently amended): A computer program storage medium readable by  
2 a computer system and encoding a computer program for executing a computer  
3 process generating a permission grant set for a code assembly received from a  
4 resource location, the computer process comprising:

5           receiving a security policy specification defining a plurality of code groups,  
6 each code group being associated with a code-group permission set;

7           receiving evidence associated with the code assembly;

8           evaluating the evidence relative to the code groups to determine  
9 membership of the code assembly in ~~one~~ two or more of the code groups; and

10          generating the permission grant set based on ~~one~~ two or more code-group  
11 permission sets, each code-group permission set of the ~~one~~ two or more code-  
12 group permission sets being associated with a code group in which the code  
13 assembly is a member.

14  
15          **26.-36.** (canceled)  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

1           37. (currently amended): A computer program product encoding a  
2 computer program for executing on a computer system a computer process for  
3 generating a permission grant set for a code assembly received from a resource  
4 location, the code assembly being associated with an evidence set, the computer  
5 process comprising:

6           receiving a security policy specification defining at least one code group  
7 collection having ~~one~~ two or more code groups, each code group being associated  
8 with a code-group permission set;

9           evaluating the evidence set relative to the code group collection to  
10 determine membership of the code assembly in ~~one~~ two or more code groups of the  
11 code group collection; and

12           generating the permission grant set based on ~~one~~ two or more code-group  
13 permission sets, each code-group permission set of the ~~one~~ two or more code-  
14 group permission sets being associated with a code group in which the code  
15 assembly is a member.

16  
17           38. (original): The program product of claim 37 wherein the generating  
18 operation comprises:

19           computing a union of the code-group permission sets associated with code  
20 groups of the code group collection in which the code assembly is a member to  
21 generate the permission grant set.

1           39. (original): The program product of claim 37 wherein the generating  
2 operation comprises:

3           selecting a code-group permission set associated with an individual code  
4 group of the code group collection in which the code assembly is a member to  
5 generate the permission grant set.

6  
7           40. (currently amended): The program product of claim 37 wherein the  
8 security policy specification further defines a plurality of policy levels associated  
9 with the ~~one~~ two or more code groups, and the generating operation comprises:

10           computing, for each policy level, a union of the code-group permission sets  
11 associated with code groups in which the code assembly is a member to generate a  
12 corresponding policy-level permission set; and

13           generating the permission grant set based on the corresponding policy-level  
14 permission set of each policy level.

15  
16           41. (currently amended): The program product of claim 40 wherein the  
17 operation of generating the permission grant set based on ~~one~~ two or more code-  
18 group permission sets further comprises:

19           computing an intersection of the corresponding policy-level permission sets  
20 associated with each policy level.

1           **42.** (currently amended): The program product of claim 40 wherein the  
2 operation of generating the permission grant set based on ~~one~~ two or more code-  
3 group permission sets further comprises:

4           computing an intersection of a subset of the corresponding policy-level  
5 permission sets.

6  
7           **43.** (original): The program product of claim 37 wherein the computer  
8 process further comprises:

9           extracting from the security policy specification a membership criterion for  
10 a code group in the plurality of code groups.

11  
12           **44.** (original): The program product of claim 43 wherein the evaluating  
13 operation comprises:

14           extracting one or more trust characteristics from the evidence;  
15           evaluating the trust characteristics relative to the membership criterion; and  
16           identifying the code assembly as a member of the code group, if the trust  
17 characteristics satisfy the membership criterion.

18  
19           **45.** (previously presented): The program product of claim 37, wherein the  
20 computer process further comprises:

21           caching the permission grant set in association with the evidence; and  
22           outputting the permission grant set in response to a subsequent receipt of  
23 the evidence without re-evaluating the evidence.

24  
25           **46.-48.** (canceled)

1  
2       **49.** (original): A method of verifying a code assembly received from a  
3 resource location, the method comprising:

4       receiving a security policy specification defining a security policy;

5       receiving evidence associated with the code assembly;

6       evaluating the evidence relative to the security policy;

7       performing verification on the code assembly;

8       detecting a verification failure of the code assembly in the operation of  
9 performing verification; and

10       determining whether the code assembly may be executed despite the  
11 verification failure, responsive to the evaluating operation.

12  
13       **50.** (original): The method of claim 49 wherein the operation of receiving  
14 evidence comprises:

15       receiving evidence associated with a class of the code assembly.

16  
17       **51.** (original): The method of claim 49 wherein the operation of receiving  
18 evidence comprises:

19       receiving evidence associated with a module of the code assembly.

20  
21       **52.** (original): The method of claim 49 wherein the operation of receiving  
22 evidence comprises:

23       receiving evidence associated with a method of the code assembly.  
24  
25

1       **53.** (previously presented): A method of verifying a code assembly  
2 received from a resource location, the method comprising:  
3       receiving a security policy specification defining a security policy;  
4       receiving evidence associated with the code assembly;  
5       evaluating the evidence relative to the security policy;  
6       generating a permission grant set, responsive to the evaluating operation;  
7       determining based on the permission grant set that a step of a verification  
8 process is unnecessary;  
9       communicating to a verification module that the step of the verification  
10 process may be bypassed;  
11       performing the verification process on the code assembly with the  
12 verification module; and  
13       bypassing the step of the verification process, responsive to the  
14 communicating operation.

15  
16       **54.** (original): The method of claim 53 wherein the generating operation  
17 comprises:  
18       generating the permission grant set in association with a module of the code  
19 assembly, responsive to the evaluating operation.

20  
21       **55.** (original): The method of claim 53 wherein the generating operation  
22 comprises:  
23       generating the permission grant set in association with a class of the code  
24 assembly, responsive to the evaluating operation.

1           **56.** (original): The method of claim 53 wherein the generating operation  
2 comprises:  
3           generating the permission grant set in association with a method of the code  
4 assembly, responsive to the evaluating operation.  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25